On the reversible extraction of classical information from a quantum source

Howard Barnum[†], Patrick Hayden[*], Richard Jozsa[†], and Andreas Winter[§]

[†]*Department of Computer Science, University of Bristol, Merchant Venturers Building, Bristol BS8 1UB U.K.*
[*]*Centre for Quantum Computation, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, U.K.*
[§]*SFB 343, Facultät für Mathematik, Universität Bielefeld, Postfach 100131, 33501 Bielefeld, Germany.*

Abstract

Consider a source $\mathcal{E}$ of pure quantum states with von Neumann entropy S. By the quantum source coding theorem, arbitrarily long strings of signals may be encoded asymptotically into S qubits/signal (the Schumacher limit) in such a way that entire strings may be recovered with arbitrarily high fidelity. Suppose that classical storage is free while quantum storage is expensive and suppose that the states of $\mathcal{E}$ do not fall into two or more orthogonal subspaces. We show that if $\mathcal{E}$ can be compressed with arbitrarily high fidelity into A qubits/signal plus any amount of auxiliary classical storage then A must still be at least as large as the Schumacher limit S of $\mathcal{E}$. Thus no part of the quantum information content of $\mathcal{E}$ can be faithfully replaced by classical information. If the states do fall into orthogonal subspaces then A may be less than S, but only by an amount not exceeding the amount of classical information specifying the subspace for a signal from the source.

1 Introduction

The quantum source coding theorem [1, 3, 2, 4, 5] provides one of the clearest manifestations of the concept of quantum information. It characterises the minimal resource (in terms of Hilbert space dimension) that is sufficient to faithfully represent long sequences of signal emissions from a memoryless quantum source. This provides a notion of the quantum information content of the source and the minimal resource is given by the Schumacher limit – S qubits/signal – where S is the von Neumann entropy of the source. In this paper we consider a possible refinement of this theorem, asking to what extent the quantum information may be represented in two parts – a classical part and a quantum part – such that the quantum part is minimised while the classical part may be as large as desired. We will show that it is impossible to reduce the resource of the quantum part to below the Schumacher limit, except in the special case that the signal states fall into two or more orthogonal subspaces. Thus in general (i.e. with the preceding exception) it is impossible to substitute classical information for any part of the quantum information of a source.

The paper is organised as follows. The main results are given in theorems 1 and 2 of section 4. We approach the proofs of these results through a sequence of lemmas after establishing some preliminary definitions and terminology. In section 2 we provide a formal definition of a coding–decoding scheme which applies to blocks of signals of general length

n. We define the fidelity of any such scheme and state Schumacher's quantum source coding theorem. In section 3 we introduce the distinction between reducible and irreducible sources i.e. sources whose signal states respectively do or do not fall into orthogonal subspaces. This distinction is fundamental for our main results and we give an alternative characterisation of it which is used in our subsequent proofs.

In section 4 we refine the concept of coding–decoding schemes to a situation in which the encoding has a classical part and a quantum part. In terms of this concept we briefly review earlier work of [8] which provided the motivation of our present study, and we give a precise statement of our main new results. For any such refined coding–decoding scheme the classical part of the encoding may be assumed to remain intact after the input signal blocks have been reconstructed (with some fidelity) by decoding. Correspondingly in section 5 we begin the proof of our main results by considering the classical mutual information $\mathcal{I}$ between the identity of the input string and the classical part of the encoding. If the input string has length n and Q denotes the number of qubits needed to support the quantum part of the encoding, then we prove that $(Q + \mathcal{I})/n$ cannot remain less than the Schumacher limit as the fidelity of the coding–decoding scheme approaches unity. Finally to provide a lower bound for Q/n, in section 6 we study the behaviour of $\mathcal{I}/n$ for irreducible and reducible sources. We prove that $\mathcal{I}/n$ must tend to zero for any irreducible source as the fidelity of the coding–decoding scheme tends to unity. For reducible sources the situation is more complicated: clearly it is possible to at least determine the identity of the orthogonal subspace to which a given signal belongs, without disturbing the signal. We prove that this is the best we can do i.e. that $\mathcal{I}/n$ cannot exceed the amount of classical information about the signal provided by this identification.

These lemmas in section 6 are mathematically precise examples of a heuristic principle in quantum information theory viz. that it is impossible to obtain information about the identity of a quantum state from an irreducible source without irreparably disturbing the state and furthermore, that there should be a trade-off between the amount of disturbance and the amount of information gained. Such information–disturbance results have been derived in other situations [9] but for us there are extra technical complications arising from the fact that the block length n must generally increase unboundedly as the fidelity of the coding–decoding scheme tends to unity i.e. we have a situation in which the source varies as the disturbance tends to zero. Our lemmas in section 6, referring to a situation of unboundedly increasing block lengths, may have a wider applicability for example to the study of the security of quantum cryptographic protocols, in which an eavesdropper may attempt to extract classical information from blocks of signal transmissions.

In section 7 we draw together the lemmas of the preceding sections to give proofs of our main results. Finally in section 8 we summarise our findings and discuss some related open questions.

2 Preliminary definitions

We begin with a more precise statement of the quantum source coding theorem which will also serve to establish terminology and notations for our main results. We sometimes denote the ensemble or source of (generally mixed) states ξ_i with prior probabilities p_i as $\{\xi_i; p_i\}$. Consider a source $\mathcal{E} = \{|\sigma_i\rangle\,; p_i\}$ of pure quantum signal states $|\sigma_i\rangle$ with prior probabilities p_i. We will use capital letter indices to denote multi-indices for blocks of signals of length n:

$$|\sigma_I\rangle = |\sigma_{i_1}\rangle \otimes \ldots \otimes |\sigma_{i_n}\rangle \tag{1}$$

$$p_I = p_{i_1} \ldots p_{i_n} \tag{2}$$

$$I = i_1 \ldots i_n \tag{3}$$

We will often write the projector $|\sigma_I\rangle\langle\sigma_I|$ simply as σ_I. Let $\mathcal{H}$ denote the Hilbert space of single signals, of dimension k, and let $\mathcal{B}_\alpha$ denote the space of all mixed states of α qubits (or the smallest integer greater than α if α is not an integer). Then n-strings σ_I are in $\mathcal{H}^{\otimes n}$ and in $\mathcal{B}_{n\log k}$. In this paper, logarithms are always to base 2.

If $|\psi\rangle$ and ρ are any pure and mixed state respectively in the same state space, we define the fidelity F by

$$F(|\psi\rangle\langle\psi|\,, \rho) = \langle\psi|\,\rho\,|\psi\rangle \tag{4}$$

More generally if ω and ρ are mixed states we define the fidelity by [13, 14]

$$F(\rho, \omega) = \left(\mathrm{tr}\,\sqrt{\sqrt{\omega}\rho\sqrt{\omega}}\right)^2 \tag{5}$$

The von Neumann entropy S of $\mathcal{E}$ is defined by

$$S = -\mathrm{tr}\,\rho\log\rho \tag{6}$$

where $\rho = \sum_i p_i\,|\sigma_i\rangle\langle\sigma_i|$ is the overall density matrix of the signal states.

An encoding-decoding scheme for blocks of length n, to α qubits/signal and average fidelity $1-\epsilon$, is defined by the following ingredients:
(i) an encoding operation $E_n : \mathcal{H}^{\otimes n} \to \mathcal{B}_{n\alpha}$ which is a completely positive trace preserving map (a CPTP map).[1] $E_n(\sigma_I)$ is a (mixed) state of $n\alpha$ qubits called the encoded or compressed version of σ_I.
(ii) a decoding operation $D_n : \mathcal{B}_{n\alpha} \to \mathcal{B}_{n\log k}$ which is also a CPTP map. We write $\tilde{\sigma}_I = D_n E_n(\sigma_I)$ and call it the decoded version of σ_I. Note that $\tilde{\sigma}_I$ is generally a mixed state.
(iii) the average fidelity between the σ_I's and $\tilde{\sigma}_I$'s is $1-\epsilon$:

$$\sum_I p_I F(\sigma_I, \tilde{\sigma}_I) = 1-\epsilon \tag{7}$$

[1] These encoding operations are called blind, in contrast to visible encodings in which E_n is allowed to be an arbitrary map, but D_n in (ii) is still required to be CPTP. See [6] for a further discussion of this distinction. Note that the visible situation is trivial for our main problem: all of the information about the input may be faithfully extracted in classical form by recording the identity of the input labels.

We say that the source $\mathcal{E}$ may be compressed to α qubits/signal if the following condition is satisfied: for all $\epsilon > 0$ there is an n_0 such that for all block lengths $n > n_0$ there is an encoding-decoding scheme for blocks of length n to α qubits/signal and average fidelity at least $1 - \epsilon$. We can now make the following precise statement.

Quantum source coding theorem. [1, 3, 2, 4] Let S be the von Neumann entropy of a source $\mathcal{E}$ of pure quantum states and suppose that $\alpha \neq S$. Then $\mathcal{E}$ may be compressed to α qubits/signal if and only if $\alpha > S$. ■

3 Reducible and irreducible sources

For our main results it will be important to classify sources according to whether or not they decompose into orthogonal parts in the following sense:

Definition 1 *A source $\mathcal{E}$ is called reducible if its signal states fall into two or more orthogonal subspaces. Otherwise $\mathcal{E}$ is called irreducible.*

If $\mathcal{E}_i = \{\alpha_{ij}; p_{ij}\}_j$ for $i = 1, \ldots, L$ are sources of signals lying in mutually orthogonal subspaces then we may construct the reducible source $\mathcal{E} = \bigcup_i a_i \mathcal{E}_i = \{\alpha_{ij}; a_i p_{ij}\}_{ij}$ where $\{a_1, \ldots, a_L\}$ is any chosen probability distribution (and the subscript outside the bracket is the index labelling the signal states). Conversely any reducible source $\mathcal{E}$ may be decomposed into irreducible parts $\mathcal{E} = \bigcup a_i \mathcal{E}_i$ by choosing a maximal orthogonal decomposition. Here a_i is the total probability of all states of $\mathcal{E}$ lying in the i^{th} orthogonal subspace and $\mathcal{E}_i$ comprises these states with suitably renormalised probabilities.

We give an alternative characterisation of irreducibility of a source of pure states which will be used in our later proofs.

Definition 2 *If $|\sigma\rangle$ and $|\tau\rangle$ are any signal states, a chain from $|\sigma\rangle$ to $|\tau\rangle$ of length m is a sequence of signal states $|\sigma_i\rangle$ beginning with $|\sigma\rangle$ and ending with $|\tau\rangle$:*

$$|\sigma\rangle = |\sigma_1\rangle, |\sigma_2\rangle \ldots, |\sigma_m\rangle = |\tau\rangle$$

such that $\langle\sigma_i|\sigma_{i+1}\rangle \neq 0$ for all $i = 1, \ldots, m-1$.

Lemma 1 *Let $\mathcal{E}$ be an ensemble with K signal states.*
(a) $\mathcal{E}$ is irreducible if and only if *for any two signal states $|\sigma\rangle$ and $|\tau\rangle$ there is a chain from $|\sigma\rangle$ to $|\tau\rangle$.*
(b) If there is a chain from $|\sigma\rangle$ to $|\tau\rangle$ then there is a chain of length at most K.

Proof We will prove the contrapositive form of (a). Thus suppose that the signal states do fall into two orthogonal subspaces E_1 and E_2. Let $|\sigma\rangle \in E_1$ and $|\tau\rangle \in E_2$. Then any chain from $|\sigma\rangle$ to $|\tau\rangle$ would have a jump from E_1 to E_2 at some stage. But this is impossible so there can be no chain from $|\sigma\rangle$ to $|\tau\rangle$. Conversely suppose that there is no chain from $|\sigma\rangle$ to $|\tau\rangle$. Let M_σ be the set of all signal states that are reachable from $|\sigma\rangle$ by chains. Let

M_σ^c be the complement. Thus $|\sigma\rangle \in M_\sigma$ and $|\tau\rangle \in M_\sigma^c$, so both sets are non-empty. Now any $|\tau'\rangle \in M_\sigma^c$ is orthogonal to all signals in M_σ (since if $\langle\sigma'|\tau'\rangle \neq 0$ for some $|\sigma'\rangle \in M_\sigma$ we would have a chain from $|\sigma\rangle$ to $|\sigma'\rangle$ that extends to $|\tau'\rangle$, which is impossible). Let E_1 and E_2 be the linear span of signals in M_σ and M_σ^c respectively. Then E_1 and E_2 are orthogonal subspaces containing all the signal states i.e. $\mathcal{E}$ is reducible.
(b) Suppose that a chain from $|\sigma\rangle$ to $|\tau\rangle$ contains some signal $|\sigma'\rangle$ twice:

$$|\sigma\rangle, \ldots, |\sigma'\rangle, \ldots, |\sigma'\rangle, \ldots |\tau\rangle .$$

Then we may delete the section between the two $|\sigma'\rangle$'s and still have a chain. Hence if there is a chain there is also a chain that contains each signal at most once i.e. having length at most K. ■
Example $\mathcal{E}$ may contain orthogonal states yet still be irreducible. Minimal chains may need to have maximal length K. Consider for example $\mathcal{E}$ with $K = 5$ states given by $|0\rangle, |0\rangle + |1\rangle, |1\rangle + |2\rangle, |2\rangle + |3\rangle, |3\rangle$. Then $\mathcal{E}$ is irreducible. $|0\rangle$ is orthogonal to $|3\rangle$ and the shortest chain between them has 5 members. ■

4 Coding with a classical and quantum part

In the context of quantum information theory, classical information may be thought of as a special case *viz* the quantum information of a source of states that are known (or required) to always be members of a prescribed orthonormal basis. More generally we may consider a quantum register as holding only classical information (relative to a prescribed orthonormal basis) if there is an omni-present fully decohering operation acting on the register, diagonal in the basis, which prevents the occurrence of any non-trivial superpositions of the basis states or any entanglements of this register with any other quantum registers being considered. Thus the most general allowable ("classical") state of the register is a probabilistic mixture of the basis states, which may be classically correlated to the quantum state of all other registers (cf eq. (8) below). These conditions endow classical information with special properties not shared by quantum information in general. For example classical information is robust compared to quantum information – it may be readily stabilised and corrected by frequent measurement in the given basis, which would destroy genuine quantum information. Also, unlike quantum information, it may be cloned or copied. These and other singular properties indicate that for many purposes it is useful to regard classical information as a separate resource, distinct from quantum information. In this vein, it is natural to ask if the quantum source coding theorem may be refined along the lines outlined in the opening paragraph of section 1 (and formulated precisely below).

Since our compression schemes are required to operate with arbitrarily high fidelity (i.e. reproduce the source states arbitrarily well as $\epsilon \to 0$) the question of whether part of the quantum information of the source may be represented in classical terms, may be alternatively phrased as the question of whether it is possible to reversibly extract classical information from a quantum source in such a way that the residual quantum information content is reduced. This question has already been raised in [8] and in [4] (at the end of chapter 1).

Consider an encoding operation E_n which encodes $|\sigma_I\rangle$ into two registers A and B where A holds the classical part and B holds the quantum part of the encoding. Let $\{|j\rangle\}$ be the classical orthonormal basis of A. The most general allowable classical state in A is a probability distribution over j values so the most general form of the encoded state may be written

$$E_n |\sigma_I\rangle = \sum_j c_j^I |j\rangle\langle j| \otimes \omega_j^I \tag{8}$$

where ω_j^I are some (generally mixed) states of the subsystem B. Here $c_j^I = p(j|I)$ is the probability of having j in A given that we are encoding the I^{th} input string. An encoding operation of this type can be physically interpreted as the action of an (incomplete) quantum measurement on $|\sigma_I\rangle$. In this case j is the measurement outcome and ω_j^I is the post measurement state (after possible further processing in a way that can depend on the value of j).

¿From p_I and $p_j = \sum_I p(j|I)p_I$ we have $p(I|j) = p(j|I)p_I/p_j$ and for each fixed value of j we get the ensemble

$$\mathcal{E}_j = \{\omega_j^I; p(I|j)\}. \tag{9}$$

Let supp_j be the least number of qubits/signal required to support the states in $\mathcal{E}_j$. Then the quantum resource of the encoding is defined to be

$$\overline{\text{supp}} = \sum_j p_j \text{ supp}_j \tag{10}$$

We will say that a source $\mathcal{E}$ may be compressed to α qubits/signal plus auxiliary classical storage if for all $\epsilon > 0$ there is an n_0 such that for all $n > n_0$ we have an encoding-decoding scheme (E_n, D_n) with fidelity $1 - \epsilon$ and $\overline{\text{supp}} = \alpha$.

In terms of the above notions the main result of [8] may be stated as follows.

Proposition 1 *([8]) Let $\mathcal{E}$ be any irreducible source of pure states. Let S be the von Neumann entropy of $\mathcal{E}$ and let E_n be any encoding scheme for blocks of length n from $\mathcal{E}$ having a classical and quantum part as in eq. (8) above. Suppose further that*
(a) the states ω_j^I in the encoding are all pure states,
(b) the coding scheme works with fidelity 1 i.e. the states $|\sigma_I\rangle$ may be perfectly *reconstituted from their encoded versions.*
Then the von Neumann entropy of each ensemble $\mathcal{E}_j$ is nS.

Hence under the assumptions (a) and (b) it is impossible to reduce the quantum resource of the encoding below the Schumacher limit S qubits/signal of the original source, by any procedure that extracts classical information, since S is also the Schumacher limit per input signal for each $\mathcal{E}_j$.

The restrictions (a) and (b) are in fact very severe. In particular a requirement of perfect fidelity (as in (b)) would rule out many basic theorems of information theory. The compression of classical information given by Shannon's source coding theorem and the compression given by the quantum source coding theorem, for example, would both be

impossible. Thus it is of great interest to require only the weaker condition of asymptotically perfect fidelity i.e. fidelity of $1-\epsilon$ for all $\epsilon > 0$ where decreasing ϵ will generally involve working with increased block lengths n. This question was raised in [8] but left open.

We now consider the most general situation where both restrictions (a) and (b) are lifted. Our main results are given in theorems 1 and 2 below.

Theorem 1 *Let $\mathcal{E} = \{|\sigma_i\rangle\,; p_i\}$ be an irreducible source of pure states with von Neumann entropy S and suppose that $\alpha \neq S$. Then $\mathcal{E}$ may be compressed to α qubits per signal plus auxiliary classical storage if and only if $\alpha > S$.*

Thus no part of the quantum information content of $\mathcal{E}$ may be represented in classical terms if $\mathcal{E}$ is irreducible. However this is no longer true if the source is reducible as shown by the following example.

Example Consider a reducible ensemble $\mathcal{E} = a_1\mathcal{E}_1 \cup a_2\mathcal{E}_2$ where $\{a_1, a_2\}$ is a probability distribution and $\mathcal{E}_i$ are irreducible, supported in orthogonal subspaces E_i respectively. If ρ_i is the density matrix of $\mathcal{E}_i$ then the density matrix ρ of $\mathcal{E}$ has a block diagonal form

$$\rho = a_1\rho_1 \oplus a_2\rho_2$$

so the Schumacher limit of $\mathcal{E}$ is

$$S(\rho) = H(a_1, a_2) + a_1 S(\rho_1) + a_2 S(\rho_2)$$

where $H(a_1, a_2)$ is the Shannon entropy of $\{a_1, a_2\}$.

We have the following encoding scheme for $\mathcal{E}$: in a long string, measure each signal (without disturbance) to determine whether it is in E_1 or E_2. This provides $H(a_1, a_2)$ bits/signal of classical information. For each value of i, Schumacher compress the signals lying in E_i to $S(\rho_i)$ qubits/signal. The total quantum resource on average[2] is $a_1 S(\rho_1) + a_2 S(\rho_2)$ qubits/signal which is less than $S(\rho)$ by the amount of the classical information extracted. Clearly the original string may be reconstituted with arbitrarily high fidelity (for suitably large block lengths) from the classical and quantum parts of the encoding. Thus if the original ensemble $\mathcal{E}$ is reducible, it is always possible to convert part of its quantum information into classical information. In theorem 2 we will see that the above scheme is actually optimal for providing the minimal quantum resources in any classical-quantum compression scheme for a reducible ensemble. ■

Theorem 2 *Let $\mathcal{E} = \bigcup_{l=1}^{L} a_l\mathcal{E}_l$ be any reducible ensemble with von Neumann entropy S where $\mathcal{E}_l$ are irreducible subensembles supported in orthogonal subspaces. Let S_l be the von Neumann entropy of $\mathcal{E}_l$ and suppose that $\alpha \neq \sum_l a_l S_l$. Then $\mathcal{E}$ may be compressed to α qubits per signal plus auxiliary classical storage if and only if*

$$\alpha > \sum_l a_l S_l = S - H(a_1, \ldots, a_L).$$

[2]To make this statement precise we need to invoke properties of typical sequences as given in the proof of theorem 2 later.

Note that if we do not require the residual quantum resource of the encoding to be smaller than that of the original source then reversible extraction of classical information (even with perfect fidelity) is always possible. Indeed as described in [8] the process of quantum teleportation may be interpreted as a scheme for encoding a quantum source into classical and quantum information with perfect fidelity in decoding, but the associated quantum resource of the encoding is not less than that of the original source. Also one may consider the trivial encoding of retaining the input string untouched and merely attaching independent classical information, which is discarded in the decoding.

We will approach the proofs of theorem 1 and theorem 2 through a series of lemmas. Firstly lemma 2 below will relate the quantum resource of any encoding-decoding scheme to the amount of mutual information per signal, between the classical part of the encoding and the identity of the input string. Then we will use lemmas 3 and 5 to show that this mutual information must tend to zero for irreducible sources, as the fidelity of the scheme tends to unity, and we will also characterise its limiting value for reducible sources.

5 Mutual information of the classical extraction

Lemma 2 *Let $\mathcal{E}$ be a source with von Neumann entropy S. Let (E_n, D_n) be any encoding-decoding scheme for blocks of length n with average fidelity $1-\epsilon$. Suppose that the encoded states have a classical and quantum part as in eq. (8). Let $\overline{\text{supp}}$ be the quantum resource of the encoding (as in eq. (10)) and let $\mathcal{I}(I:J)$ denote the mutual information between the input string I and the classical data j i.e. the mutual information of the probability distribution $p(I\&j) = p_I\, c_j^I$. Then*

$$\overline{\text{supp}} + \frac{\mathcal{I}(I:J)}{n} \geq S - f(\epsilon) \tag{11}$$

where $f(\epsilon)$ is a function satisfying

$$f(\epsilon) \to 0 \qquad as \qquad \epsilon \to 0.$$

Remark We will actually prove a slightly stronger statement. Let (E, D) be an encoding-decoding scheme for a source $\mathcal{E}_{in}$ in dimension d with von Neumann entropy S_{in}. Let $\overline{\text{Supp}}$ be the average number of qubits needed to support the intermediate ensembles $\mathcal{E}_j$ and let I denote the identity of the input state. Then

$$\overline{\text{Supp}} + \mathcal{I}(I:J) \geq S_{in} - f(\epsilon)\log d \tag{12}$$

In lemma 2, $\mathcal{E}_{in}$ has the form $\mathcal{E}^{\otimes n}$ (i.e. n-strings from $\mathcal{E}$) so $S_{in} = nS$, $\overline{\text{Supp}} = n\overline{\text{supp}}$ and $d = k^n$ where k is the dimension of the single signal space.

Proof Let us write the encoded states as

$$\tau_I = E_n\,|\sigma_I\rangle = \sum_j p(j|I)\,|j\rangle\langle j| \otimes \omega_j^I. \tag{13}$$

These states all have a block diagonal form with blocks labelled by j containing $p(j|I)\omega_j^I$. Consider the ensemble $\mathcal{E}_{enc} = \{\tau_I; p_I\}$. The average state is $\overline{\tau} = \sum_I p_I \tau_I$ and the Holevo quantity of $\mathcal{E}_{enc}$ is

$$\chi_{enc} = S(\overline{\tau}) - \sum_I p_I S(\tau_I).$$

If we fix on any single value of j we have the ensemble $\mathcal{E}_j = \{\omega_j^I; p(I|j)\}$. Let χ_j be the Holevo quantity of $\mathcal{E}_j$. Using the block diagonal form of $\mathcal{E}_{enc}$ a straightforward rearrangement of the formula for χ gives

$$\chi_{enc} = \sum_j p_j \chi_j + \mathcal{I}(I:J). \tag{14}$$

For any ensemble the Holevo quantity satisfies $\chi \leq \log d$ where d is the dimension of the space of states for the ensemble. Hence

$$\chi_j \leq n \text{ supp}_j \qquad \text{for all } j. \tag{15}$$

and from eqs. (15) and (14)

$$n \overline{\text{supp}} + \mathcal{I}(I:J) \geq \chi_{enc}. \tag{16}$$

Now consider the decoding stage. We have

$$D_n(\tau_I) = \tilde{\sigma}_I$$

with average fidelity

$$\overline{F} = \sum_I p_I F(|\sigma_I\rangle, \tilde{\sigma}_I) = 1 - \epsilon.$$

Let χ_{dec} be the Holevo quantity of the decoded ensemble $\mathcal{E}_{dec} = \{\tilde{\sigma}_I; p_I\}$ and let $\chi_{in} = nS$ be the Holevo quantity of the input ensemble $\mathcal{E} = \{|\sigma_I\rangle; p_I\}$. We will use the result, proved in appendix A, that high fidelity ensembles have close χ's. More precisely, since $\mathcal{E}_{in}$ and $\mathcal{E}_{dec}$ (supported in dimension $d = k^n$ where k is the dimension of the single signal space) have fidelity $1 - \epsilon$ we can say

$$|\chi_{in} - \chi_{dec}| \leq 4(\sqrt{\epsilon}\log(k^n) - \sqrt{\epsilon}\log(2\sqrt{\epsilon})) \tag{17}$$

so

$$\chi_{dec} \geq nS - 4n\sqrt{\epsilon}\log k + 4\sqrt{\epsilon}\log(2\sqrt{\epsilon}) \tag{18}$$

Now the decoding operation D_n is a CPTP map and by the Uhlmann-Lindblad monotonicity theorem [10, 11] the Holevo quantity is non-increasing under any CPTP map. Thus $\chi_{enc} \geq \chi_{dec}$ and eqs. (16) and (18) give

$$n \overline{\text{supp}} + \mathcal{I}(I:J) \geq nS - 4n\sqrt{\epsilon}\log k + 4\sqrt{\epsilon}\log(2\sqrt{\epsilon})$$

so

$$\overline{\text{supp}} + \frac{\mathcal{I}(I:J)}{n} \geq S - f(\epsilon)$$

where $f(\epsilon) \to 0$ as $\epsilon \to 0$, as required. ■

6 An information–disturbance relation

To complete the proof of theorem 1 we will argue that $\mathcal{I}(I:J)/n$ must also tend to zero as ϵ tends to zero. The intuitive reason is the following. After encoding and decoding (thinking of ϵ as being very small) the states $\tilde{\sigma}_I$ reproduce the states $|\sigma_I\rangle$ with high fidelity. But the classical data j can be assumed to remain after the process since it may be copied at the encoding stage into another register which is not affected by the decoding operation. Now it is a general heuristic principle in quantum physics that one cannot obtain information about a fixed source of non-orthogonal states without disturbing them and furthermore there should be a tradeoff between the amount of disturbance and the amount of information gained. The fundamental role of information-disturbance tradeoffs in quantum measurement theory has been emphasised by C. A. Fuchs [9]. However we need a more refined version of this principle as our input source generally varies (because of increasing block lengths) as the disturbance ϵ tends to zero. Nevertheless we will show that $\mathcal{I}(I:J)/n$, the information gained per signal, goes to zero as the fidelity approaches 1.

Indeed in the limiting case of perfect fidelity (i.e. where $\tilde{\sigma}_I = |\sigma_I\rangle\langle\sigma_I|$) it is not difficult to show that $\mathcal{I}(I:J)$ must be exactly zero (cf [12]). The proof is as follows: Any CPTP map may be represented as a unitary operation acting on the input together with an ancilla (in some standard initial state $|0\rangle$) followed by tracing over a subsystem of the output. Thus the encoding and decoding operation on $|\sigma_I\rangle$ may be represented as a unitary operation U on $|\sigma_I\rangle_A |0\rangle_B$ in registers A and B where B is the ancilla, yielding a pure state

$$U(|\sigma_I\rangle_A |0\rangle_B) = |\lambda_I\rangle_{AB}$$

where $\tilde{\sigma}_I = \mathrm{tr}_B |\lambda\rangle\langle\lambda|$ and the classical data is obtained from a subsystem of $\mathrm{tr}_A |\lambda\rangle\langle\lambda|$. If the $|\sigma_I\rangle$'s are reproduced with perfect fidelity we must have

$$|\lambda\rangle_{AB} = |\sigma_I\rangle_A |\psi_I\rangle_B$$

for some pure states $|\psi_I\rangle$. But then from the unitarity of U

$$\langle\sigma_I|\sigma_K\rangle\langle 0|0\rangle = \langle\sigma_I|\sigma_K\rangle\langle\psi_I|\psi_K\rangle.$$

Hence if there is a chain from $|\sigma_I\rangle$ to $|\sigma_K\rangle$ we must have $\langle\psi_I|\psi_K\rangle = 1$ i.e. $|\psi_I\rangle = |\psi_K\rangle$. If $\mathcal{E}$ is irreducible then this is true for all I and K so no measurement on register B can yield any information about the identity of I. In particular $\mathcal{I}(I:J)$ must be zero.

In lemmas 3 and 5 below we will generalise the above argument to the scenario of arbitrarily high (but not perfect) fidelity, showing that $\mathcal{I}(I:J)/n \to 0$ as $\epsilon \to 0$.

Lemma 3 *Suppose that $\mathcal{E} = \{|\sigma_i\rangle\,; p_i\}$ is an irreducible source with K states. Suppose that the states $|\sigma_i\rangle$ are provided in a register A with state space $\mathcal{B}_{\alpha_1}$ and let register B be an ancilla with state space $\mathcal{B}_{\alpha_2}$. We will refer to B as the environment. Let*

$$\Gamma : \mathcal{B}_{\alpha_1} \otimes \mathcal{B}_{\alpha_2} \to \mathcal{B}_{\alpha_1} \otimes \mathcal{B}_{\alpha_2} \tag{19}$$

$$\Gamma\,|\sigma_i\rangle_A |0\rangle_B = |\xi_i\rangle_{AB} \tag{20}$$

be a unitary map such that

$$\sum_i p_i F\left(|\sigma_i\rangle, \text{tr}_B |\xi_i\rangle\langle\xi_i|\right) = 1 - \epsilon \tag{21}$$

Let $\{\rho_i = \text{tr}_A |\xi_i\rangle\langle\xi_i| ; p_i\}$ *be the environment ensemble and let*

$$\chi = S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i)$$

be the Holevo quantity of the environment. Then if $\mathcal{E}$ *is kept fixed but* ϵ, Γ *and* α_2 *are allowed to vary, we have* $\chi \leq f(\epsilon)$ *where the function* f *satisfies* $f(\epsilon) \to 0$ *as* $\epsilon \to 0$. *In fact we may take* $f(\epsilon) = A\sqrt{\epsilon} + B\sqrt{\epsilon}\log\sqrt{\epsilon}$ *where* A *and* B *are constants.*

Remark We are thinking here of Γ as being a unitary extension of a CPTP coding-decoding map $D_n E_n$ with high fidelity $1 - \epsilon$. Note that any coding–decoding scheme for any source may be assumed to be of the form Γ in eq. (19) where register A contains the final decoded state and the environment B may, without loss of generality, be assumed to retain a copy of the classical part of the encoding (since it may be copied after encoding and the copy kept intact during decoding). Thus $\text{tr}_B |\xi_i\rangle\langle\xi_i|$ is the decoded version of the input $|\sigma_i\rangle$ and by Holevo's theorem [15] χ of the environment is an upper bound for the amount of information about i that may be obtained by any measurement on B. Thus the lemma states that any such information must approach zero as the average disturbance to the ensemble tends to zero.

The proof of lemma 3 is given in appendix B.

Note that in lemma 3 the source is kept constant as ϵ varies: there is no notion of increasing block length as $\epsilon \to 0$. For our desired application in theorem 1 the ensemble $\mathcal{E}$ varies as $\epsilon \to 0$ since the block length generally increases. The proof of lemma 3 is not directly applicable in this situation (as the parameters K and ζ also increase with block length) and this extra complication is dealt with in lemma 5 below. As a preliminary result we have:

Lemma 4 (Markov Lemma) *Let* $\{X_i; p_i\}$ *be any random variable with* $0 \leq X_i \leq 1$ *and mean* $\overline{X} > 1 - \epsilon$. *Then for any* A *we have* $Prob(X_i < 1 - A\epsilon) < \frac{1}{A}$. *In particular*

$$Prob(X_i < 1 - \sqrt{\epsilon}) < \sqrt{\epsilon}.$$

Proof If $Prob(X_i < 1 - A\epsilon) = \alpha$ we get

$$1 - \epsilon < \sum p_i X_i = \sum_{X_i < 1 - A\epsilon} p_i X_i + \sum_{X_i \geq 1 - A\epsilon} p_i X_i \leq (1 - A\epsilon)\alpha + (1 - \alpha)1 = 1 - A\alpha\epsilon$$

Hence $A\alpha < 1$. ■.

Lemma 5 *Suppose we have a sequence* $\{\epsilon_m > 0\}$ *with* $\epsilon_m \to 0$ *and let* $n(m)$ *be any (generally unbounded) function of* m. *Suppose also that for each* m *we have:*

(i) a source $\mathcal{E}^{(m)} = \mathcal{E}_1^{(m)} \otimes \ldots \otimes \mathcal{E}_{n(m)}^{(m)}$ *where each* $\mathcal{E}_i^{(m)}$ *is an irreducible source on a state space of at most* k *dimensions with at most* K *signal states.*
(ii) An encoding-decoding scheme $(E^{(m)}, D^{(m)})$ *on* $\mathcal{E}^{(m)}$ *with average fidelity* $1-\epsilon_m$*, leaving the environment in a state* $\rho_I^{(m)}$ *for input state labelled by* $I = i_1 \ldots i_{n(m)}$*.*
Then $\chi(\{\rho_I^{(m)}; p_I^{(m)}\})/n(m) < g(\epsilon_m)$ *where* g *is a function satisfying* $g(\epsilon) \to 0$ *as* $\epsilon \to 0$*. Hence the amount of information per position tends to zero as the fidelity tends to 1, for arbitrarily changing block lengths in the schemes.*

Remark In our application below of lemma 5 to an irreducible ensemble $\mathcal{E}$, $\mathcal{E}^{(m)}$ will be the ensemble of strings of length $n(m)$ from $\mathcal{E}$ so $\mathcal{E}_i^{(m)} = \mathcal{E}$ for all i and m. For reducible ensembles $\mathcal{E}$ however, it will be necessary to consider the irreducible parts of the ensemble of $n(m)$-strings so that each $\mathcal{E}_i^{(m)}$ will range over the various irreducible subensembles of $\mathcal{E}$ and we will need lemma 5 in its full generality.

Proof of lemma 5 Let us fix attention on any one of the schemes labelled by m and omit reference to the value of m in all labels, for notational clarity. We write $I_{\neq l}$ for the input string with the l^{th} position deleted.

Let $\tau_{i_1 \ldots i_n}$ be the decoded output for the input string $|\sigma_{i_1 \ldots i_n}\rangle = |\sigma_{i_1}\rangle \ldots |\sigma_{i_n}\rangle \in \mathcal{E}_1 \otimes \ldots \mathcal{E}_n$ and write

$$F_I \equiv F_{i_1 \ldots i_n} = \langle \sigma_{i_1 \ldots i_n} | \, \tau_{i_1 \ldots i_n} \, | \sigma_{i_1 \ldots i_n} \rangle \, .$$

Let $p_I \equiv p_{i_1 \ldots i_n} = p_{i_1}^{(1)} \ldots p_{i_n}^{(n)}$ where $p_i^{(k)}$ is the probability of $|\sigma_i\rangle$ in the ensemble $\mathcal{E}_k$. For notational clarity we will henceforth omit the superscript (k) on the probabilities. Then

$$F = \sum_{i_1 \ldots i_n} p_{i_1 \ldots i_n} F_{i_1 \ldots i_n} = 1 - \epsilon. \tag{22}$$

Let $\{\rho_I; p_I\}$ be the ensemble of final environment states of the coding–decoding scheme. We will use the following inequality, proved in appendix C, for the Holevo quantity of the environment:

$$\frac{\chi(\{\rho_I; p_I\})}{n} \leq \max_k \sum_{I_{\neq k}} p_{I_{\neq k}} \chi_{I_{\neq k}}, \tag{23}$$

where

$$\chi_{I_{\neq k}} = S(\sum_{i_k} p_{i_k} \rho_I) - \sum_{i_k} p_{i_k} S(\rho_I)$$

and we will argue that each term on the RHS of eq. (23) tends to zero with ϵ.

Consider $k = 1$ (all others are similar). For each fixed choice of $I_{\neq 1} = i_2 \ldots i_n$ we extend $|\sigma_i\rangle$ in the I_1 slot by $|\sigma_{i_2 \ldots i_n}\rangle$, apply the operation DE, and look at the I_1 slot of the output. This is a coding/decoding of $|\sigma_i\rangle$ (i.e. length 1 string from $\mathcal{E}_1$) with output $\tau_i = \text{tr}_{\, i_2 \ldots i_n} \tau_{i i_2 \ldots i_n}$. Furthermore $\chi_{I_{\neq 1}}$ is the Holevo quantity of the environment after this coding–decoding of $\mathcal{E}_1$. The fidelity is

$$\begin{aligned} F^{(i_2 \ldots i_n)} &= \textstyle\sum_i p_i \, \langle \sigma_i | \, \tau_i \, | \sigma_i \rangle \\ &= \textstyle\sum_i p_i \, \langle \sigma_i | \, \text{tr}_{\, i_2 \ldots i_n} \tau_{i i_2 \ldots i_n} \, | \sigma_i \rangle \\ &\geq \textstyle\sum_i p_i \, \langle \sigma_{i i_2 \ldots i_n} | \, \tau_{i i_2 \ldots i_n} \, | \sigma_{i i_2 \ldots i_n} \rangle = \sum_i p_i F_{i i_2 \ldots i_n} \end{aligned} \tag{24}$$

(Here the last inequality arises since we can extend $|\sigma_{i_2\ldots i_n}\rangle$ to an orthonormal basis of the $I_2 \ldots I_n$ slots to perform the partial trace.)

Next we apply the Markov lemma to the random variable

$$\{X_{i_2\ldots i_n} \equiv F^{(i_2\ldots i_n)} = \sum_i p_i F_{ii_2\ldots i_n}\,;\, p_{i_2\ldots i_n}\}$$

(noting that eq. (22) gives $\overline{X} > 1-\epsilon$) to conclude:

$$\sum_i p_i F_{ii_2\ldots i_n} < 1-\sqrt{\epsilon} \quad \text{with probability} < \sqrt{\epsilon}.$$

Divide strings $i_2 \ldots i_n$ (taken with probabilities $p_{i_2\ldots i_n}$) into

$$S_{good} = \{i_2 \ldots i_n | \sum_i p_i F_{ii_2\ldots i_n} > 1-\sqrt{\epsilon}\} \quad \text{with total probability} > 1-\sqrt{\epsilon}$$

$$S_{bad} = \{i_2 \ldots i_n | \sum_i p_i F_{ii_2\ldots i_n} < 1-\sqrt{\epsilon}\} \quad \text{with total probability} < \sqrt{\epsilon}$$

i.e. S_{good} are those extensions of I_1 which retain high fidelity for reproducing the first slot after coding/decoding of the extension. Now

$$\sum_{I_{\neq 1}} p_{I_{\neq 1}} \chi_{I_{\neq 1}} = \sum_{good}(same) + \sum_{bad}(same).$$

For good sequences, lemma 3 then gives $\chi_{I_{\neq 1}} \leq f(\sqrt{\epsilon})$ (as fidelity of the coding/decoding is $> 1-\sqrt{\epsilon}$) where f is a function satisfying $f(x) \to 0$ as $x \to 0$. For bad sequences we always have $\chi_{I_{\neq 1}} \leq \log k$, where k is the dimension of the one-signal space. This is because for each value of $I_{\neq 1}$ the ensemble $\{\rho_{i_1 i_2\ldots i_n}; p_{i_1}\}_{i_1}$ is obtained by a CPTP map from $\{|\sigma_{i_1}\rangle\,; p_{i_1}\}$ so from the Uhlmann-Lindblad monotonicity theorem we get $\chi_{I_{\neq 1}} \leq \chi(\mathcal{E}_1) \leq \log k$.

Hence from the weights of the good and bad sets we get

$$\chi_{I_{\neq 1}} \leq (1-\sqrt{\epsilon}) f(\sqrt{\epsilon}) + \sqrt{\epsilon}\log k \equiv g(\epsilon)$$

where clearly $g(\epsilon) \to 0$ as $\epsilon \to 0$. ■.

7 Completing the main proofs

Finally we assemble our lemmas to provide proofs of theorems 1 and 2.

Proof of theorem 1 Suppose that $\mathcal{E}$ can be compressed to α qubits/signal plus auxiliary classical storage. Then for each $\epsilon > 0$ and all sufficiently large n there is an encoding-decoding scheme which, by lemma 2 satisfies

$$\alpha + \frac{\mathcal{I}(I:J)}{n} \geq S - f(\epsilon). \tag{25}$$

Here $f(\epsilon) \to 0$ as $\epsilon \to 0$ and by lemma 5 (with $\mathcal{E}_i = \mathcal{E}$ for all i) we have $\mathcal{I}(I:J)/n \to 0$ as $\epsilon \to 0$ too. But eq. (25) holds for all $\epsilon > 0$ so if $\alpha \neq S$ we must have $\alpha > S$.

Conversely if $\alpha > S$ then $\mathcal{E}$ may be compressed to α qubits/signal using just standard Schumacher compression (and no auxiliary classical storage). ■

For the proof of theorem 2 we will use the following standard result:

Lemma 6 (Lemma of typical sequences) *[16] Let $\mathcal{P} = \{p_1, \ldots, p_L\}$ be any probability distribution and consider sequences $i_1 \ldots i_n$ of the symbols $1, \ldots, L$ with probabilities $p_{i_1} \ldots p_{i_n}$. Let $n(i)$ be the number of times that the symbol i occurs in the sequence. For any $\epsilon > 0$ and n let $S_n(\epsilon) = \{i_1 \ldots i_n : |n(i) - np_i| < L\frac{\sqrt{n}}{\sqrt{\epsilon}}\}$. Then for any $\epsilon > 0$ there is an n_0 such that for all $n > n_0$ the total probability of $S_n(\epsilon)$ is greater than $1 - \epsilon$. For such sufficiently large n, $S_n(\epsilon)$ is called a set of ϵ-typical sequences.*

Thus a sequence is typical if the frequency of occurrence of each symbol i in it is approximately equal to the prior probability p_i.

Proof of theorem 2 We have a signal ensemble $\mathcal{E} = \bigcup_{l=1}^{L} a_l \mathcal{E}_l$ where $\mathcal{E}_l$ are irreducible ensembles supported in orthogonal subspaces. Let $\mathcal{A}$ denote the probability distribution $\{a_1, \ldots, a_L\}$.

Suppose that $\mathcal{E}$ can be compressed into α qubits per signal plus auxiliary classical storage. Then for each $\epsilon > 0$ and all sufficiently large n there is an encoding-decoding scheme for n-strings with fidelity $F > 1 - \epsilon$ and $\overline{\text{supp}} = \alpha$.

The source of all n-strings from $\mathcal{E}$ decomposes into irreducible parts:

$$\mathcal{E}^{\otimes n} = \bigcup_{l_1 \ldots l_n} a_{l_1} \ldots a_{l_n} \mathcal{E}_{l_1} \otimes \ldots \otimes \mathcal{E}_{l_n}$$

and the fidelity may be expressed as an average:

$$F = \sum_{l_1 \ldots l_n} a_{l_1} \ldots a_{l_n} F_{l_1 \ldots l_n} > 1 - \epsilon$$

where $F_{l_1 \ldots l_n}$ is the fidelity of the scheme when restricted to $\mathcal{E}_{l_1} \otimes \ldots \otimes \mathcal{E}_{l_n}$. We will apply lemmas 2 and 5 to these irreducible parts. For any sequence $l_1 \ldots l_n$ let $n(l)$ denote the number of times that the symbol $l = 1, \ldots L$ occurs. Then the von Neumann entropy of $\mathcal{E}_{l_1} \otimes \ldots \otimes \mathcal{E}_{l_n}$ is $\sum_l n(l) S_l$.

By applying the Markov lemma to the random variable $\{F_{l_1 \ldots l_n}; a_{l_1} \ldots a_{l_n}\}$ we obtain a set of sequences

$$S_{good} = \{l_1 \ldots l_n : F_{l_1 \ldots l_n} > 1 - \sqrt{\epsilon}\} \quad \text{with total probability} > 1 - \sqrt{\epsilon}$$

By selecting the ϵ-typical subset of these we get

$$S_{good,typ} = \{l_1 \ldots l_n : F_{l_1 \ldots l_n} > 1 - \sqrt{\epsilon} \ \text{ and } l_1 \ldots l_n \text{ is } \epsilon\text{-typical}\}$$

with total probability $> 1 - 2\sqrt{\epsilon}$.

Consider the compression scheme acting on the irreducible component $\mathcal{E}_{l_1} \otimes \ldots \otimes \mathcal{E}_{l_n}$. For any one of the good sequences lemma 2 gives

$$n\alpha + \mathcal{I}(I_{l_1 \ldots l_n} : J) \geq \sum_l n(l) S_l - nf(\sqrt{\epsilon})$$

where $\mathcal{I}(I_{l_1 \ldots l_n} : J)$ is the mutual information for the source of restricted n-strings and $f(x) \to 0$ as $x \to 0$. Furthermore lemma 5 gives $\mathcal{I}(I_{l_1 \ldots l_n} : J)/n < g(\sqrt{\epsilon})$ where $g(x) \to 0$ as $x \to 0$ too. Hence

$$\alpha \geq \sum_l \frac{n(l)}{n} S_l - f(\sqrt{\epsilon}) - g(\sqrt{\epsilon})$$

If our chosen good sequence is also typical then

$$a_l - \frac{L}{\sqrt{\epsilon}\sqrt{n}} < \frac{n(l)}{n} < a_l + \frac{L}{\sqrt{\epsilon}\sqrt{n}}$$

so for each fixed ϵ, $\frac{n(l)}{n} \to a_l$ as $n \to \infty$. Thus

$$\alpha \geq \sum_l a_l S_l - f(\sqrt{\epsilon}) - g(\sqrt{\epsilon})$$

and finally letting $\epsilon \to 0$ we get $\alpha \geq \sum a_l S_l$ as required.

Conversely to see that the bound is tight let $\epsilon > 0$ and $\delta > 0$ be any chosen values and let $\alpha = \sum_l a_l S_l + \delta$. For all sufficiently large n we encode an n-string from $\mathcal{E}^{\otimes n}$ as follows. We first measure each signal (without disturbance) to determine which sub-ensemble $\mathcal{E}_l$ it belongs to, giving a string $l_1 \ldots l_n$ drawn from $\mathcal{A}^n$. If the sequence $l_1 \ldots l_n$ is ϵ-typical for $\mathcal{A}$ (so each value l occurs between $a_l n \pm L\sqrt{n}/\sqrt{\epsilon}$ times) we perform Schumacher compression to $na_l S_l + O(\sqrt{n})$ qubits for each value of l, giving $\sum a_l S_l + O(\frac{1}{\sqrt{n}})$ qubits/signal overall. If the string is atypical we generate an arbitrary fixed state of $n\alpha$ qubits. By the dominating weight of typical sequences and the asymptotic fidelity of Schumacher compression, this scheme clearly has fidelity $1 - O(\epsilon)$ and for all sufficiently large n, the quantum resource will be less than $\alpha = \sum a_l S_l + \delta$ qubits/signal. ■

8 Concluding remarks

We have shown that no part of the quantum information of an irreducible source may be replaced by classical information if arbitrarily long strings are to be reconstitutable with asymptotically high fidelity $1 - \epsilon$ for all $\epsilon > 0$. Also for reducible sources we have characterised the maximum possible amount of classical information that can be reversibly extracted from the source under the above conditions.

To obtain these results we first proved some information–disturbance relations. Let $\mathcal{E}$ be an irreducible source. If some mutual information $\mathcal{I}$ is obtained about the identity of the state from a single emission from $\mathcal{E}$ by any physical process, leaving the state intact with average fidelity $1 - \epsilon$ then we showed that $\mathcal{I} \to 0$ as $\epsilon \to 0$. For strings of length n

from $\mathcal{E}$ we considered a sequence of encoding-decoding schemes (labelled by $m = 1, 2, \ldots$) with asymptotically perfect fidelity ($1 - \epsilon_m \to 1$) for which the string length $n(m)$ may vary arbitrarily (e.g. grow unboundedly) with m. In this case we showed that the mutual information *per letter* $\mathcal{I}_m/n(m)$ provided by the m^{th} scheme, must tend to zero as the fidelity tends to 1. This was sufficient for our purposes but raises the interesting question of a possibly stronger result: does $\mathcal{I}_m$ itself necessarily tend to zero too, as $\epsilon_m \to 0$, or can $\mathcal{I}_m$ remain nonzero under these conditions (while $\mathcal{I}_m/n \to 0$)? Consider for example an irreducible source $\mathcal{E} = \{|\sigma_0\rangle, |\sigma_1\rangle; p_0, p_1\}$ of two non-orthogonal states. Is it possible to have a sequence of encoding-decoding schemes (E_n, D_n) for strings of increasing length n, such that the n^{th} scheme has average fidelity $1 - \epsilon_n$ with $\epsilon_n \to 0$ and the n^{th} scheme provides $\mathcal{I}_n = 1$ bit of information about the identity of the string? Here $\mathcal{I}_n/n \to 0$ so our result is not contradicted yet a nonzero amount of information about the whole string is obtained with vanishing disturbance to the states. This question remains open.

Acknowledgements

RJ is supported by the U.K. Engineering and Physical Sciences Research Council and PH is supported by the Rhodes Trust. AW is supported by SFB 343 "Diskrete Strukturen in der Mathematik" of the Deutsche Forschungsgemeinschaft. Part of this work was carried out during collaborative visits supported by the European Science Foundation. HB, PH and RJ also acknowledge the support of the European 5^{th} framework network QAIP IST-1999-11234.

Appendix A

Proposition 2 *Let $\mathcal{E}_1 = \{\omega_k; p_k\}$ and $\mathcal{E}_2 = \{\rho_k; p_k\}$ be two ensembles on the same space, of dimension d, with the same prior probabilities. Here ω_k and ρ_k are generally mixed states. Let χ_1 and χ_2 be their Holevo quantities. Suppose*

$$\overline{F} = \sum_k p_k F(\omega_k, \rho_k) = 1 - \epsilon$$

with $\epsilon \leq 1/16$. Then

$$|\chi_1 - \chi_2| \leq 4(\sqrt{\epsilon} \log d - \sqrt{\epsilon} \log(2\sqrt{\epsilon}) \tag{26}$$

Proof In [7] it is shown that

$$|\chi_1 - \chi_2| \leq 2(\epsilon' \log d - \epsilon' \log \epsilon') \tag{27}$$

where

$$\sum_i p_i ||\omega_i - \rho_i|| = \epsilon' \leq \frac{1}{2}$$

and $||\omega||$ denotes the trace norm (i.e. the sum of the absolute values of the eigenvalues) of ω. This norm is related to our fidelity function by [4, 18]

$$||\rho - \omega|| \leq 2\sqrt{1 - F(\rho, \omega)}.$$

Let $\epsilon_k = 1 - F(\rho_k, \omega_k)$. Then

$$\epsilon' = \sum p_k ||\omega_k - \rho_k|| \leq 2 \sum p_k \sqrt{\epsilon_k} \leq 2\sqrt{\sum p_k \epsilon_k} = 2\sqrt{\epsilon}. \tag{28}$$

Thus if $\epsilon \leq \frac{1}{16}$ we have $\epsilon' \leq \frac{1}{2}$ and eqs. (27) and (28) give the required inequality eq. (26). ■

We note that a slightly weaker form of eq. (26) is proved by different means in [6].

Appendix B

Proof of lemma 3 Let η be the smallest non-zero overlap $|\langle \sigma_i | \sigma_j \rangle|$ of any two signals $|\sigma_i\rangle$ and $|\sigma_j\rangle$. We have

$$\Gamma : \mathcal{B}_{\alpha_1} \otimes \mathcal{B}_{\alpha_2} \to \mathcal{B}_{\alpha_1} \otimes \mathcal{B}_{\alpha_2}$$

mapping $|\sigma_i\rangle_A |0\rangle_B$ to $|\xi_i\rangle_{AB}$. Write

$$\tilde{\sigma}_i = \text{tr}_B |\xi_i\rangle\langle\xi_i| .$$

The average fidelity is

$$\overline{F} = \sum_i p_i F(|\sigma_i\rangle, \tilde{\sigma}_i) = 1 - \epsilon.$$

For each i let $F(|\sigma_i\rangle, \tilde{\sigma}_i) = 1 - \epsilon_i$ so that

$$\sum_i p_i \epsilon_i = \epsilon \tag{29}$$

Since we have $\mathcal{E}$ fixed but may think of ϵ as varying, we have $\epsilon_i = O(\epsilon)$ for each i.

For each value of i we consider an orthonormal basis of register A which has $|\sigma_i\rangle$ as its first member:

$$\{|\sigma_i\rangle, |\tau_1\rangle, |\tau_2\rangle, \ldots\}.$$

Since $|\xi_i\rangle$ has fidelity $1 - \epsilon_i$ to be $|\sigma_i\rangle$ in register A, we can write:

$$|\xi_i\rangle_{AB} = \sqrt{1 - \epsilon_i}\, |\sigma_i\rangle_A |\beta_i\rangle_B + \sqrt{\epsilon_i}\, |\gamma_i\rangle_{AB} \tag{30}$$

where the normalised state $|\gamma_i\rangle_{AB}$ has the form

$$|\gamma_i\rangle = \sum_{m \geq 1} a_m |\tau_m\rangle |\delta_m\rangle \tag{31}$$

and $|\beta_i\rangle, |\delta_1\rangle, |\delta_2\rangle, \ldots$ are some normalised states of B (which generally all vary with i). For any other value k of i we have correspondingly

$$|\xi_k\rangle_{AB} = \sqrt{1 - \epsilon_k}\, |\sigma_k\rangle_A |\beta_k\rangle_B + \sqrt{\epsilon_k}\, |\gamma_k\rangle_{AB} . \tag{32}$$

Our strategy is the following: thinking of ϵ_i and ϵ_k as small we note that the $|\gamma\rangle_{AB}$ terms have small amplitude and we will now argue that the states $|\beta_i\rangle$ and $|\beta_k\rangle$ are then also close. Hence the reduced states in register B for different values of i will be almost independent

of i and hence will have very low χ. Correspondingly any measurement on B can provide only very little information about the identity of i. For notational clarity we will sometimes write the product state $|\alpha\rangle\,|\beta\rangle$ of registers AB as $|\alpha\beta\rangle$.

The unitarity of Γ with the expressions eqs. (30) and (32) gives

$$\langle\sigma_i|\sigma_k\rangle\langle 0|0\rangle = \langle\xi_i|\xi_k\rangle = \sqrt{1-\epsilon_i}\sqrt{1-\epsilon_k}\,\langle\sigma_i|\sigma_k\rangle\,\langle\beta_i|\beta_k\rangle + \tag{33}$$

$$\sqrt{1-\epsilon_i}\sqrt{\epsilon_k}\,\langle\sigma_i\beta_i|\,\gamma_k\rangle + \sqrt{1-\epsilon_k}\sqrt{\epsilon_i}\,\langle\gamma_i|\,\sigma_k\beta_k\rangle + \sqrt{\epsilon_i}\sqrt{\epsilon_k}\,\langle\gamma_i|\gamma_k\rangle. \tag{34}$$

Each inner product in the last three terms is a complex number with modulus at most one. Let us denote them by a_1, a_2 and a_3 and write $\mu = \langle\sigma_i|\sigma_k\rangle$. Then

$$\sqrt{1-\epsilon_i}\sqrt{1-\epsilon_k}\langle\beta_i|\beta_k\rangle = 1 - \frac{(\sqrt{1-\epsilon_i}\sqrt{\epsilon_k}\,a_1 + \sqrt{1-\epsilon_k}\sqrt{\epsilon_i}\,a_2 + \sqrt{\epsilon_i}\sqrt{\epsilon_k}\,a_3)}{\mu}. \tag{35}$$

Now if ϵ is sufficiently small we will have

$$\left|\frac{\sqrt{\epsilon_i}}{\mu}\right| < \frac{1}{3} \qquad \text{and} \qquad \left|\frac{\sqrt{\epsilon_k}}{\mu}\right| < \frac{1}{3}$$

and recalling that $|a_i| \leq 1$ we have

$$\left|\frac{(\sqrt{1-\epsilon_i}\sqrt{\epsilon_k}\,a_1 + \sqrt{1-\epsilon_k}\sqrt{\epsilon_i}\,a_2 + \sqrt{\epsilon_i}\sqrt{\epsilon_k}\,a_3)}{\mu}\right|$$
$$\leq \frac{(\sqrt{1-\epsilon_i}\sqrt{\epsilon_k} + \sqrt{1-\epsilon_k}\sqrt{\epsilon_i} + \sqrt{\epsilon_i}\sqrt{\epsilon_k})}{\mu} \leq 1.$$

Also $\sqrt{\epsilon_i}\sqrt{\epsilon_k} \leq \frac{\sqrt{\epsilon_i}+\sqrt{\epsilon_k}}{2}$ and $\mu \geq \eta$ for all non-orthogonal $|\sigma_i\rangle$ and $|\sigma_k\rangle$. Putting all this together with eq. (35) we see that for all non-orthogonal pairs $|\sigma_i\rangle$ and $|\sigma_k\rangle$ we have

$$|\langle\beta_i|\beta_k\rangle| \geq 1 - \frac{3(\sqrt{\epsilon_i}+\sqrt{\epsilon_k})}{2\eta} \equiv 1 - \zeta' \tag{36}$$

and note that $\zeta' = O(\sqrt{\epsilon})$. Hence we can write

$$|\beta_k\rangle = (1-\zeta)\,|\beta_i\rangle + \sqrt{2\zeta-\zeta^2}\,\left|\beta_{ik}^{\perp}\right\rangle \tag{37}$$

where $\langle\beta_i|\beta_{ik}^{\perp}\rangle = 0$ and $\zeta = O(\sqrt{\epsilon})$ so $|\beta_k\rangle \to |\beta_i\rangle$ as $\epsilon \to 0$.

Recalling eq. (30) and using eq. (37) in eq. (32) we have

$$\begin{aligned} |\xi_i\rangle &= \sqrt{1-\epsilon_i}\,|\sigma_i\rangle\,|\beta_i\rangle + \sqrt{\epsilon_i}\,|\gamma_i\rangle \\ &\equiv \sqrt{1-\epsilon_i}\,|\sigma_i\rangle\,|\beta_i\rangle + O(\sqrt{\epsilon}) \qquad (38) \\ |\xi_k\rangle &= \sqrt{1-\epsilon_k}(1-\zeta)\,|\sigma_k\rangle\,|\beta_i\rangle + \sqrt{\zeta}\sqrt{(2-\zeta)}\sqrt{1-\epsilon_k}\,|\sigma_k\rangle\,\left|\beta_{ik}^{\perp}\right\rangle + \sqrt{\epsilon_k}\,|\gamma_k\rangle \\ &\equiv \sqrt{1-\epsilon_k}\,|\sigma_k\rangle\,|\beta_i\rangle + O(\sqrt{\epsilon}) \qquad (39) \end{aligned}$$

Now write

$$\text{tr}_{\,A}\,|\xi_i\rangle\langle\xi_i| = \Omega_i.$$

Let us modify $|\xi_i\rangle$ into $|\xi_i'\rangle$ by replacing the basis $\{|\sigma_i\rangle, |\tau_1\rangle, |\tau_2\rangle, \ldots\}$ in eqs. (30) and (31) by the corresponding basis $\{|\sigma_k\rangle, |\tau_1'\rangle, |\tau_2'\rangle, \ldots\}$ used in the expression for $|\xi_k\rangle$. Then $|\xi_k\rangle$ is a purification of Ω_k and $|\xi_i'\rangle$ is still a purification of Ω_i. Thus for all $\langle\sigma_i|\sigma_k\rangle \neq 0$, we have

$$F(\Omega_i, \Omega_k) \geq |\langle\xi_i'|\xi_k\rangle|^2 \geq 1 - O(\sqrt{\epsilon}).$$

Now $\mathcal{E}$ with K states is irreducible so by lemma 7 there is a chain of length at most K from $|\sigma_{i_0}\rangle$ to every other $|\sigma_j\rangle$. Hence for every j, Ω_j is near to any chosen Ω_{i_0} in the following sense:

$$F(\Omega_{i_0}, \Omega_j) \geq 1 - K\,O(\sqrt{\epsilon}). \tag{40}$$

We now compare the constant ensemble $\mathcal{E}_{const} = \{\Omega_{i_0}; p_i\}$ having $\chi(\mathcal{E}_{const}) = 0$, with the actual ensemble $\mathcal{E} = \{\Omega_i; p_i\}$ of reduced states in register B arising from Γ, having $\chi(\mathcal{E}) = \chi$. From eq. (40) we have

$$\overline{F}(\mathcal{E}_{const}, \mathcal{E}) = 1 - KO(\sqrt{\epsilon})$$

and the result in appendix A gives $|\chi - 0| \leq f(\epsilon)$ where $f(\epsilon)$ has the form $A\sqrt{\epsilon} + B\sqrt{\epsilon}\log\sqrt{\epsilon}$ for suitable constants A and B, and $f(\epsilon) \to 0$ when $\epsilon \to 0$, as required. ■

Appendix C

We use the notation I to denote the index string $I = i_1 \ldots i_n$ and $I_{\neq k}$ to denote the string I with the k^{th} position deleted. We aim to prove:

Lemma 7 *Let $p_I = p_{i_1}^{(1)} \ldots p_{i_n}^{(n)}$ be any product distribution of n probability distributions and let $\{\rho_I; p_I\}$ be any associated ensemble of quantum states. Then*

$$\chi(\{\rho_I; p_I\}) \leq n \max_k \sum_{I_{\neq k}} p_{I_{\neq k}} \left[S(\sum_{i_k} p_{i_k}\rho_I) - \sum_{i_k} p_{i_k} S(\rho_I) \right] \tag{41}$$

We begin by defining the conditional and mutual entropies for a quantum state σ_{ABC} on three systems A, B and C:

$$\begin{aligned} S(A|B) &= S(A,B) - S(B) && (42)\\ S(A:B) &= S(A) + S(B) - S(A,B) && (43)\\ S(A:B|C) &= S(A|C) + S(B|C) - S(A,B|C). && (44) \end{aligned}$$

Here $S(A)$, $S(A,B)$ etc. denote the von Neumann entropies of the states of the designated subsystems, obtained by partial trace from σ_{ABC}. The following chain rules for conditional and mutual entropies are then simple consequences of the definitions:

$$\begin{aligned} S(A_1, A_2, \ldots, A_n|B) &= \sum_k S(A_k|A_{<k}, B) && (45)\\ S(A_1, A_2, \ldots, A_n : B) &= \sum_k S(A_k : B|A_{<k}). && (46) \end{aligned}$$

(where $A_{<k}$ denotes the list $A_1, \ldots, A_{k-1}$). Now suppose we are given a state $\sigma_{A_1 A_2 \ldots A_n B}$ such that $\sigma_{A_1 A_2 \ldots A_n} = \sigma_{A_1} \otimes \ldots \otimes \sigma_{A_n}$. We can calculate, for example, that

$$\begin{aligned} S(A_2 : B|A_1) &= S(A_2|A_1) + S(B|A_1) - S(A_2, B|A_1) && (47) \\ &= S(A_1) + S(A_1, B) - S(A_1) - S(A_1, A_2, B) + S(A_1) && (48) \\ &= S(A_2 : A_1, B). && (49) \end{aligned}$$

This relationship can then be used to prove an upper bound on the joint quantum mutual entropy as in the proposition below. This bound is a quantum analogue of a classical mutual information inequality given in [17].

Proposition 3 *For a state $\sigma_{A_1 A_2 \ldots A_n B}$ such that $\sigma_{A_1 A_2 \ldots A_n} = \sigma_{A_1} \otimes \ldots \otimes \sigma_{A_n}$ the following inequality holds:*

$$S(A_1, A_2, \ldots, A_n : B) \leq n \max_k S(A_k : A_{\neq k}, B). \tag{50}$$

Proof

$$\begin{aligned} S(A_1, A_2, \ldots, A_n : B) &= \sum_k S(A_k : B|A_{<k}) && (51) \\ &= \sum_k S(A_k : A_{<k}, B) && (52) \\ &= \sum_k S(A_k : \mathrm{tr}_{>k} A_{\neq k}, B) && (53) \\ &\leq \sum_k S(A_k : A_{\neq k}, B) && (54) \\ &\leq n \max_k S(A_k : A_{\neq k}, B). && (55) \end{aligned}$$

The next to last inequality follows from the strong subadditivity of von Neumann entropy, which implies that the quantum mutual entropy cannot increase under any CPTP map. ■

To obtain our desired inequality for χ, we specialize to the case where A is a classical system correlated with B. Let

$$\sigma_{A_1 A_2 \ldots A_n B} = \sum_I p_I \left|I\right\rangle\!\left\langle I\right|_A \otimes \rho_B^I \tag{56}$$

where $I = i_1 i_2 \ldots i_n$, $p_I = \prod_{k=1}^n p_{i_k}^{(k)}$ and $\left|I\right\rangle = \otimes_{k=1}^n \left|i_k\right\rangle_{A_k}$ for sets of orthogonal states $\{\left|i_k\right\rangle_{A_k}\}$. Then a straightforward calculation gives

$$\begin{aligned} S(A_1, A_2, \ldots, A_n : B) &= S(\sum_I p_I \rho_I) - \sum_I p_I S(\rho_I) && (57) \\ &= \chi(\{p_I; \rho_I\}) && (58) \end{aligned}$$

and applying the proposition gives

$$\chi(\{\rho_I; p_I\}) \leq n \max_k \sum_{I_{\neq k}} p_{I_{\neq k}} \left[S(\sum_{i_k} p_{i_k} \rho_I) - \sum_{i_k} p_{i_k} S(\rho_I) \right], \tag{59}$$

as required.

References

[1] B. W. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, pp. 2738–2747, 1995.

[2] H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher, "General fidelity limit for quantum channels," *Physical Review A*, vol. 54, pp. 4707, 1996.

[3] R. Jozsa and B. W. Schumacher, "A new proof of the quantum noiseless coding theorem," *Journal of Modern Optics*, vol. 41, pp. 2343–2349, 1994.

[4] A. Winter, PhD thesis, "Coding theorems of quantum information theory" , Chapter 1, available at quant-ph/9907077.

[5] R. Jozsa, M. Horodecki, P. Horodecki and R. Horodecki, "Universal quantum information compression", *Phys. Rev. Lett.* **81**, pp. 1714-1717, 1998.

[6] H. Barnum, C. Caves, C. A. Fuchs, R. Jozsa and B. Schumacher, "On quantum coding for ensembles of mixed states", quant-ph/0008024

[7] M. Horodecki, "Limits for compression of quantum information carried by ensembles of mixed states", *Phys. Rev.* **A** 57, p 3364, 1998.

[8] C. H. Bennett, G. Brassard, R. Jozsa, D. Mayers, A. Peres, B. Schumacher and W. Wootters, "Reduction of quantum entropy by reversible extraction of classical information", *J. Mod. Optics*, **41**, p2307-2314 (1994).

[9] C. A. Fuchs, "Information gain vs. state disturbance in quantum theory", *Fortschritte der Physik* **46** pp. 535-566, 1998.

[10] G. Lindblad, "Entropy, information, and quantum measurements," *Communications in Mathematical Physics*, vol. 33, pp. 305–322, 1973.

[11] A. Uhlmann, "Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory," *Communications in Mathematical Physics*, vol. 54, pp. 21–32, 1977.

[12] C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum cryptography wthout Bell's theorem", *Phys. Rev. Lett.* **68**, pp. 557-559, 1992.

[13] A. Uhlmann, "The "transition probability" in the state space of a *-algebra," *Reports on Mathematical Physics*, vol. 9, pp. 273–279, 1976.

[14] R. Jozsa, "Fidelity for mixed quantum states," *Journal of Modern Optics*, vol. 41(12), pp. 2314–2323, 1994.

[15] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel", *Probl. Peredachi Inf.* **9**, pp. 3-11, 1973.

[16] T. Cover and J. Thomas, "Elements of Information Theory", Wiley, New York 1991.

[17] E. Biham, M. Boyer, P.O. Boykin, T. Mor and V. Roychowdhury, "A proof of the security of quantum key distribution", appendix H1. Preprint available at quant-ph/9912053.

[18] C. A. Fuchs and J. van de Graaf "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Transactions on Information Theory*, vol. 45, pp. 1216–1227, 1999.